UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,203	11/09/2000	Hideki Koike	LEXW116493	4596

26389 7590 09/15/2006

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/710,203
Filing Date: November 09, 2000
Appellant(s): KOIKE ET AL.

Shoko I. Leek
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed June 26, 2006 appealing from the Office action mailed March 22, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

The appellant's statement of the grounds of rejection includes a statement stating whether Claims 1-6, 8-21, and 23-36 are unpatentable under 35 U.S.C. 103(a) over Shen (U.S. Patent No. 6,611,850) in view of Falkner (U.S. Patent No. 5,713,008). This grounds of rejection had been withdrawn in the previous Office Action mailed March 22, 2006, and is therefore, no longer an issue for review under appeal. The only remaining

grounds of rejection is the 35 U.S.C. 102(a) rejection over Schneier et al. ("Cryptographic Support for Secure Logs on Untrusted Machines").

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Schneier, Bruce. "Cryptographic Support for Secure Logs on Untrusted Machines", January 1998, Seventh USENIX Security Symposium Proceedings, USENIX Press, pp. 53-62.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1 and 26 rejected under 35 U.S.C. 102(a). These rejections are fully set forth in a prior Office action mailed March 22, 2006.

Claims 1 and 26 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier et al. ("Cryptographic Support for Secure Logs on Untrusted Machines").

Regarding claim 1, Schneier discloses:

A log file protection system for protecting log files in which computer system operations have been recorded, comprising:

log file creation means which create a plurality of identical log files which record the operations of said computer systems (Section 3.2: paragraph 1; Section 4.2: paragraphs 8-11), wherein it is stated that "U_o should log the data in several parallel logfiles, with each logfile using a different untrusted server as its trusted server";

alteration detection means which periodically monitor said plurality of identical log files for alteration or deletion (Section 1: paragraphs 4, 9-11, Section 3.3: paragraph 1; Section 3.4: paragraph 1); and

restoration means which restore the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected by said alteration detection means (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup.

Regarding claim 26, Schneier discloses:

A log file protection method for protecting log files in which computer system operations have been recorded, comprising:

(a) creating a plurality of identical log files which record the operations of said computer system systems (Section 3.2: paragraph 1; Section 4.2: paragraphs 8-11), wherein it is stated that "U_o should log the data in several parallel logfiles, with each logfile using a different untrusted server as its trusted server";

(b) periodically monitoring said plurality of identical log files for alteration or deletion (Section 1: paragraphs 4, 9-11, Section 3.3: paragraph 1; Section 3.4: paragraph 1); and

(c) restoring the altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected in said periodic monitoring step (Section 5: paragraph 1), wherein the log file can be replaced with a clean backup.

(10) Response to Argument

The Appellant's arguments regarding the rejection under 35 U.S.C. 103(a) over Shen (U.S. Patent No. 6,611,850) in view of Falkner (U.S. Patent No. 5,713,008), are not addressed in the following arguments, as the rejection has already been withdrawn in the Office action mailed on March 22, 2006.

The Appellant has argued:

That Schneier does not teach, "periodically monitoring the plurality of identical log files for alteration or deletion." In particular, the appellant argues that Schneier does not teach the monitoring of the plurality of identical log files for alteration or deletion.

The Examiner contends that Schneier does teach periodically monitoring a plurality of identical log files for alteration or deletion as claimed in claims 1 and 26. Schneier teaches a method which prevents an attacker from undetectably modifying or destroying a log file (see Abstract). The system disclosed by Schneier teaches a system wherein a untrusted machine which creates a log file communicates with either one trusted machine or a plurality of untrusted machines to check if the created log files have changed (see Section 3.1, Section 4.2). Schneier states that "we only need U to

communicate the log entries to T infrequently, at some period related to the frequency which you expect T may be comprised" (See Section 1: paragraph 11). This ***periodic*** communication between U (the untrusted machine creating the log files) and T (the trusted machine) is for the purpose of checking to see if the log files have been changed or destroyed. This interaction between U and T, maybe also be between U and a plurality of untrusted machines as seen in Section 4.2. Furthermore, in the embodiment with the untrusted machine U communicating with a plurality of untrusted machines to detect the change or deletion of any log files, the untrusted machine should "log the same data in several parallel logfiles, with each logfile using a different untrusted server as its trusted server" (Section 4.2). These several parallel logfiles with the same data are analogous to the identical log files as claimed in claims 1 and 26. Therefore the communication between the untrusted machine and the one or more servers is periodic, multiple identical log files are created and stored, and the periodic interaction between the untrusted machine and the one or more servers determines if a log file is changed or deleted. Therefore, the Examiner contends that Schneier does teach, "periodically monitoring the plurality of identical log files for alteration or deletion."

The Appellant further argues:

That Schneier does not teach, "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files."

The Examiner contends that Schneier does teach, "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files."

Schneier teaches a system of monitoring log files and detecting if a log file has been changed or deleted by communication between the logging machine and one or more of other machines. Schneier teaches storing a plurality of identical log files (Section 4.2). Furthermore, Schneier teaches that A_o, a log file, can be stored on n untrusted machines, and if A_o is deleted, that A_o can be recovered from any m of the machines (Section 4.2, page 8: column 2). Furthermore, Schneier states that if a log file has been compromised, that the user can "restore it from a clean backup" (Section 5, paragraph 1). Therefore, it is asserted that Schneier does teach, "replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files."

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

K.A. 9/08/06
KA 09/06/2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu KV

Kambiz Zand